

VŠB – Technická univerzita Ostrava  
Fakulta elektrotechniky a informatiky  
Katedra informatiky

---

# **Absolvování individuální odborné praxe**

## **Individual Professional Practice in the Company**

2012

Lukáš Durdák

VŠB - Technická univerzita Ostrava  
Fakulta elektrotechniky a informatiky  
Katedra informatiky

## Zadání bakalářské práce

Student:

**Lukáš Durd'ák**

Studijní program:

B2647 Informační a komunikační technologie

Studijní obor:

2612R025 Informatika a výpočetní technika

Téma:

Absolvování individuální odborné praxe  
Individual Professional Practice in the Company

Zásady pro vypracování:

1. Student vykoná individuální praxi ve firmě: Tieto Czech s.r.o.
2. Struktura závěrečné zprávy:
  - a) Popis odborného zaměření firmy, u které student vykonal odbornou praxi a popis pracovního zařazení studenta.
  - b) Seznam úkolů zadaných studentovi v průběhu odborné praxe s vyjádřením jejich časové náročnosti.
  - c) Zvolený postup řešení zadaných úkolů.
  - d) Teoretické a praktické znalosti a dovednosti získané v průběhu studia uplatněné studentem v průběhu odborné praxe.
  - e) Znalosti či dovednosti scházející studentovi v průběhu odborné praxe.
  - f) Dosažené výsledky v průběhu odborné praxe a její celkové zhodnocení.

Seznam doporučené odborné literatury:

Podle pokynů konzultanta, který vede odbornou praxi studenta.

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **doc. Ing. Michal Krátký, Ph.D.**

Konzultant bakalářské práce: Mgr. Přemysl Pavlošek

Datum zadání: 18.11.2011

Datum odevzdání: 04.05.2012



doc. Dr. Ing. Eduard Sojka  
vedoucí katedry



prof. RNDr. Václav Snášel, CSc.  
děkan fakulty

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě 2. května 2012



.....

Rád bych na tomto místě poděkoval zástupcům společnosti Tieto Czech s.r.o, za možnost absolvovat zde praxi a rovněž celému odbornému týmu, že mi byli vždy nápomocni a rádi s čímkoliv pomohli.

## **Abstrakt**

Tato bakalářská práce se zabývá popisem procesů probíhajících ve firmě Tieto Czech s ohledem na práci na oddělení správy Unixových serverů a virtualizace, kterou jsem vykonával. Obsahuje popis vybrané skupiny problémů a jejich řešení ať už teoretické tak i praktické. Dále jsou zde uvedené informace o získaných znalostech a zkušenostech.

**Klíčová slova:** Unix, Linux, HP-UX, Solaris, AIX, VMWare, virtualizace, praxe, administrace, LVM, DRBD, klastr

## **Abstract**

This thesis shows overview of processes in Tieto Czech s.r.o company, with focus on work in Unix and Virtualisation team which I have done. It describes selected group of problems and their solutions – theoretical or practical. Also it contains description of my archived experience and knowledge.

**Keywords:** Unix, Linux, HP-UX, Solaris, AIX, VMWare, virtualization, professional practice, administration, LVM, DRBD, cluster

## Seznam použitých zkratek a symbolů

VLAN	– Virtuální LAN dle IEEE 802.1q
PXE	– Preboot Execution Environment
DHCP	– Dynamic Host Configuration Protocol, protokol pro dynamickou konfiguraci IP adresy hosta
FTP	– File Transfer Protocol, protokol používaný k přenosu souborů
SSH	– Secure Shell, protokol pro síťové zprostředkování příkazového řádku
runlevel	– úroveň operativní funkčnosti Unixového systému, každý runlevel obsahuje předdefinovanou skupinu funkcionalit
LVM	– Logical Volume Manager, správce logických oddílů disků
NIC	– Network Interface Card, zařízení síťové karty
RHEV	– Redhat Enterprise virtualizace
VM	– Virtual Machine, virtuální stroj

## Obsah

<b>1</b>	<b>Úvod</b>	<b>5</b>
1.1	Seznámení s prostředím . . . . .	5
1.2	Struktura týmu . . . . .	6
1.3	Rozsah architektury . . . . .	6
<b>2</b>	<b>Prostředí</b>	<b>7</b>
2.1	Problem Management . . . . .	7
2.2	Change Management . . . . .	8
<b>3</b>	<b>Prostředky pro práci</b>	<b>9</b>
3.1	SSH, tunely a přístupy . . . . .	9
3.2	Citrix XenApp . . . . .	10
3.3	Monitoring . . . . .	11
3.4	Tikety . . . . .	12
3.5	Virtualizace . . . . .	13
<b>4</b>	<b>Řešené úkoly - UNIX</b>	<b>16</b>
4.1	Plný souborový systém . . . . .	16
4.2	Rozšíření místa na disku . . . . .	16
4.3	Spadlé procesy, služby . . . . .	17
4.4	Správa uživatelských účtů . . . . .	18
4.5	Audit . . . . .	19
4.6	Instalace nových serverů . . . . .	20
4.7	Cluster . . . . .	21
4.8	DRBD . . . . .	21
4.9	Pacemaker, Corosync a RedHat Cluster Suite . . . . .	22
4.10	Veritas Cluster . . . . .	23
<b>5</b>	<b>Řešené úkoly - Virtualizace</b>	<b>24</b>
5.1	Alokace . . . . .	24
5.2	Reporty . . . . .	24
5.3	Migrace serverů . . . . .	24
5.4	Nové prostředí a P2V konverze . . . . .	25
5.5	Disaster recovery, MIM . . . . .	25
<b>6</b>	<b>Zákazníci a soft skills</b>	<b>26</b>
<b>7</b>	<b>Zhodnocení praxe</b>	<b>27</b>
7.1	Znalosti uplatněné . . . . .	27
7.2	Scházející znalosti a zkušenosti . . . . .	27
<b>8</b>	<b>Závěr</b>	<b>28</b>

<b>Přílohy</b>	<b>29</b>
<b>A Přílohy k práci</b>	<b>30</b>
A.1 Pracovní deník . . . . .	30



## Seznam obrázků

1	Úvodní obrazovka SSH Klienta PuTTY . . . . .	10
2	Citrix ICA Client . . . . .	10
3	Rozhraní Patrol Central Operator . . . . .	11
4	Rozhraní nástroje BMC Remedy User . . . . .	12
5	Hypervizor typu 1 (bare-metal) . . . . .	13
6	Hypervizor typu 2 . . . . .	13
7	Schéma funkcionality DRBD . . . . .	21

---

## Seznam výpisů zdrojového kódu

1	Manuální řešení problému plného disku . . . . .	16
2	Rozšíření LVM oddílu . . . . .	17
3	Přidání zařízení VG . . . . .	17
4	Přidání prostoru při použití ZFS . . . . .	17
5	Část skriptu pro vytváření uživatelů . . . . .	18
6	Část skriptu řešící připojení na server . . . . .	19
7	Úsek konfigurace služby RedHat Clusteru . . . . .	22
8	Přidání služby apache do clusteru . . . . .	23
9	Vytvoření seznamu virtuálního prostředí pomocí PowerCli . . . . .	24
10	Migrate serverů mezi úložišti . . . . .	25

## 1 Úvod

Společnost Tieto Czech s.r.o [11] je mezinárodní IT společnost s dlouhou historií. Vznikla v roce 1968 ve Finsku. Původní název společnosti je Tietotehdas Oy a její působnost byla omezena pouze na lokální zákazníky z odvětví bankovníctví a lesního průmyslu, kterým zajišťovala chod sálových počítačů. Následně s rostoucím všeobecným zájmem o IT odvětví se působnost firmy rozšířila i na osobní počítače a vývoj softwaru. V 90. letech 20. století došlo k rychlému rozvoji oboru což mělo vliv i na rychlý růst společnosti. V roce 1995 byl změněn název společnosti na TT Tieto o dva roky později pouze na Tieto. V této době byla působnost firmy rozšířena rovněž na oblast telekomunikací. Od roku 1999 začla společnost používat obchodní název TietoEnator. Ten vycházel z názvů dvou společností – Tieto a nově připojené švédské partnerské společnosti Enator. Zhruba v této době došlo rovněž k rozšíření působnosti společnosti na trhy mimo Finsko. Od března 2009 společnost opět používá snadněji zapamatovatelný název Tieto.

Významným počinem bylo otevření pobočky v České Republice, ke kterému došlo v roce 2004 akvizicí firmy Sikora. Z původních několika málo zaměstnanců se rozrostlo české zastoupení na současných přibližně 1500 zaměstnanců pracujících v různých oborech.

V současnosti společnost Tieto zaměstnává po celém světě přibližně 18000 odborníků a poskytuje své služby v oblastech telekomunikace, média, finanční služby, automobilový průmysl, energetika, dřevozpracující průmysl, zdravotnictví a sociální péče, průmyslová výroba, obchod, logistika a veřejná správa mnoha zákazníkům převážně ve skandinávských zemích. V brzké době je plánována expanze na Ruský trh a do Německa.

### 1.1 Seznámení s prostředím

Svou praxi jsem vykonával v týmu zabývajícím se správou a implementací Unixových řešení a virtualizace na platformách X86.

Česká pobočka Tietu zahrnuje tři na sobě nezávislé na Unix zaměřené týmy, přičemž jeden má svou působnost rozšířenu rovněž na platformu virtualizace. Toto rozložení odpovídá historickému modelu rozdělení týmů orientovaných na různá odvětví. První tým spravuje pouze systémy poskytující finanční služby, státní služby a zdravotnictví. Druhý tým má na starost zákaznické systémy z oblastí obchod, logistika, průmyslová výroba a příbozná odvětví. Tým, do kterého jsem zařazen já má, na starost telekomunikace, média a interní služby Tietu – které zhruba od poloviny roku 2009 zahrnují i virtualizaci.

Týmy platformy úzce spolupracují s jinými týmy majícími na starost další služby. Jedním z takových týmů je skupina zabývajícím se správou a alokací diskových polí. Ti musí zajistit správný chod diskových systémů a jejich alokaci a viditelnost pro Unixové a virtualizační servery. Další významný tým je tým síťové podpory, který zajišťuje bezchybný provoz většiny síťových zařízení. Za zmínku stojí uvést, že většina síťových prvků použitých v infrastruktuře je značky Cisco, případně Juniper. Jelikož data uložená na serverech musí být chráněna proti ztrátě, případně uložena bezpečně dle zákonů desítky let, existuje rovněž tým zabývajícím se zálohováním. Z významných týmů stojí

rovněž za zmínku skupina zabývající se řešením a zúsobů monitorování služeb a serverů. Kromě Unixových platforem existují rovněž i specifické týmy zabývající se správou operačních systémů na bázi Microsoft Windows.

## 1.2 Struktura týmu

Unixový tým, ve kterém jsem prováděl praxi se skládá z 15 lidí. Ti jsou rozděleni na pracovníky ve směnném provozu a na ty, jež dělají jen denní směny. Jelikož denní směny mají pokrývat většinu práce, jsou tito lidé dále rozděleni podle architektur, popřípadě zákazníků tak aby každý denní pracovník měl nějakou část své působnosti. Pracovníci na směnném provozu nejsou takto úzce profilováni. Směny jsou nastaveny do osmisměnného provozu a probíhají po 7,5 hodinách denní a odpolední směna a 12 hodin noční směny. Já byl zařazen do denního provozu, se zaměřením primárně na virtualizaci serverů a několika externích zákazníků z oboru Unixu.

## 1.3 Rozsah architektur

Architektury, s nimiž se můžeme setkat při práci v týmu Unix jsou následující:

- Unixové systémy
  - Redhat Enterprise Linux, x86 a x86\_64
  - SuSe Linux Enterprise Server, x86 a x86\_64
  - SuSe Linux Enterprise Desktop, x86 a x86\_64
  - Debian, Ubuntu, a jiné deriváty
  - Sun Solaris, Oracle Solaris, Sparc a x86
  - HP-UX (Hewlett Packard)
  - AIX (IBM)
  - Tru64
- Virtualizace
  - VMware vSphere, ESX, ESXi, 4.0 a výš (x86\_64)
  - VMware Infrastructure, ESX, ESXi, 3.5 a nižší (x86)
  - Citrix XEN
  - RedHat RHEV 3
  - Oracle VM

Virtualizace byla zařazena k Unixovu především z důvodů historických. První virtualizační nástroje byly vytvořeny pouze pro Linux, popřípadě měly v základech skryto Linuxové jádro. V dnešní době ovšem mnoho součástí nástrojů pro virtualizaci pokrývá spíše platformy Windows. Úspěšný administrátor tak musí znát více platforem.

## 2 Prostředí

Všechny postupy ve firmě odpovídají předem definovaným procesům dle ITIL. Práce na pozici Unixového specialisty zahrnuje Monitoring and Control management, který je rozdělen na:

- Incident management
- Problem management
- Change management

a nachází se na druhé a třetí vrstvě třívrstvého modelu.

První vrstva (Tier) pokrývá především monitoring a řešení jednoduchých úkolů. O to se stará tým nazvaný **ControlDesk**. Dalším úkolem první vrstvy je kontakt s koncovými uživateli. Ten obstarává oddělení nazývané **ServiceDesk**. Na ty se ve společnosti Tieto můžeme obracet buďto telefonicky, přes email nebo přes interní aplikaci MySupport. První vrstva obecně rovněž působí jako jakési síto, které propustí jen opravdu relevantní požadavky a problémy na další vrstvy. Například chvilkové přetížení monitorovací soustavy, popřípadě nesmyslný požadavek od uživatele je zde uzavírán a není eskalován na další úroveň podpory.

Druhá vrstva se stará o odborné řešení problémů a požadavků, které se nedaly vyřešit na první vrstvě podpory. Předpokládá se zde jistá úroveň znalostí a zkušeností pracovníků. Druhá vrstva obvykle nemá přímý přístup k hardware.

Na třetí vrstvu by pak měly proniknout už jen velmi sofistikované problémy, neřešitelné na první vrstvě především z Problemového nebo Change managementu. Nyní se ovšem práce druhé a třetí vrstvy velice překrývá.

Dále je do práce specialisty zahrnut i Projektový management. Ten pokrývá návrh, plánování a implementaci architektur nových prostředí a obsahuje procesy nutné k jeho úspěšné realizaci a překlopení do fáze udržovací, tj. Monitoring and Control.

### Incident Managemet

Vše v této oblasti se týká řešení jednorázových, neopakujících se požadavků od koncových uživatelů, či z automatického monitoringu serverů – takzvaných incidentů. Incident je pak definován jako událost, jež není součástí běžného provozu a může způsobit výpadek, nebo omezení služeb.

#### 2.1 Problem Managemet

Cílem Problémového managementu je předcházet vzniku událostí, které povedou opakovaně ke vzniku incidentů. Tedy většinou dojde k vytvoření problému na reakci na několik neustále se opakujících incidentů. Výstupem problémového managementu by měla být změna – change, která problém vyřeší.

## **2.2 Change Managemet**

Má za úkol nastavit sadu procesů nutných k provedení netriviální změny v infrastruktuře. Vyžaduje pečlivé plánování a obvykle i rezervaci lidských a výpočetních zdrojů, či schválení koncovým zákazníkem, či uživatelem. Může být výsledkem problémového managementu, ale není to nutně podmínkou. Změny mohou vnikat rovněž i na požadavek zákazníků.

### 3 Prostředky pro práci

Jelikož je většina z serverů umístěna ve skandinávských zemích a nemůžeme k nim přistupovat přímo, používá se jejich správě několik rozličných metod vzdáleného přístupu.

Z důvodů zajištění maximální bezpečnosti jsou servery ve společnosti Tieto chráněny firewally a na servery se se přistupuje skrz dedikované konzolové servery, takzvané Jump Pointy. Přes ty se dále můžeme připojovat buďto na další Jump Pointy, nebo již na konkrétní servery.

K připojení k Jump Pointům z pracovní stanice specialisty se používá zabezpečené spojení pomocí VPN, přes které následně proudí veškerá komunikace.

#### 3.1 SSH, tunely a přístupy

Základní metodou pro přístup k serveru je protokol SSH, obsažený ve většině moderních Unixových systémech. SSH nám zajišťuje bezpečnou komunikaci mezi počítači. Umožňuje přístup k příkazovému řádku vzdáleného systému. Rovněž jej můžeme použít pro kopírování souborů mezi servery, pomocí rozšíření protokolu SSH+SCP, nebo pro jakýkoliv obecný přenos dat pomocí metody zvané tunelování. Tunelování je technika, při které je zapouzdřeno jedno nebo více síťových spojení do jiného síťového spojení, v tomto konkrétním případě do již aktivního spojení SSH se serverem. Tunelování je celkem používanou metodou pokud se potřebujeme připojit na nějakou službu zabezpečenou firewallem a jediný propouštěný port je pro službu SSH. V takovém případě vytvoříme tunel skrz aktivní spojení SSH. Příkladem takového spojení může být protunelování „grafiky“, tedy protokolů VNC popřípadě X-serveru skrz SSH.

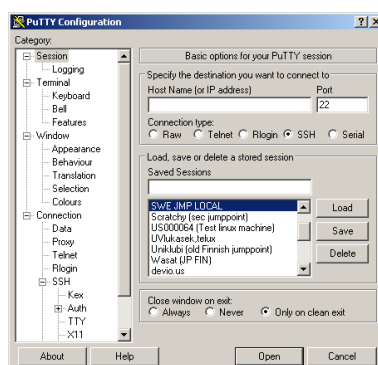
Bezpečnost protokolu SSH je zajištěna transparentním šifrováním, autentizací klienta a volitelnou kompresí dat.

Nejčastějšími používanými klienty pro tento způsob přístupu je program PuTTY [13] z prostředí Windows (obrázek 1), popřípadě řádkový OpenSSH klient v Linuxových distribucích.

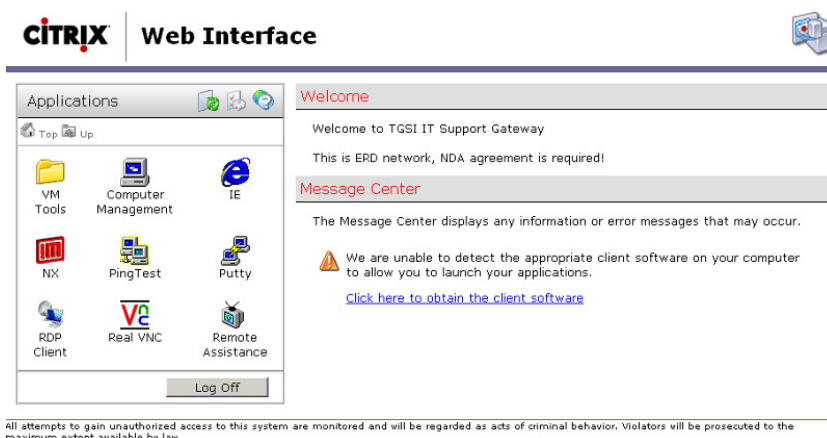
Další metodou přístupu na server je použití protokolu RDP, tedy vzdálené grafické plochy. Tato metoda je používána výhradně pro přístup k serverům s operačním systémem založeným na platformě Windows.

Jinou možností připojení na server je přístup přes integrovaný kontrolér vzdáleného přístupu. Ten je integrován přímo v hardwaru serverů a umožňuje zobrazení a monitoring stavů serveru. Možnosti se liší od výrobců konkrétního hardware. Například firma IBM nabízí ve svých serverech kontrolér IMM, dříve nazývaný ILO umožňující plnou kontrolu nad serverem z webového prohlížeče tak, jako by jsme byli u serveru fyzicky přítomni. Můžeme si prohlédnout výstupy na obrazovku v plné grafické formě, připojit obraz CD přes síť, nebo server například restartovat.

Poslední používaný přístup na servery se týká pouze serverů virtuálních. Zde se používají metody konkrétního hypervisoru a obvykle vyžadují nutnost mít nainstalován další software. Za zmínku stojí tři nejpoužívanější. U společnosti VMware se používá přístup přes software VMware VSphere klient. Firma Red-Hat pro její virtualizaci zvolila přístup přes svobodný protokol SPICE, plně integrující podporu vzdáleného přístupu



Obrázek 1: Úvodní obrazovka SSH Klienta PuTTY



Obrázek 2: Citrix ICA Client

a firma Citrix používá pro svůj produkt XenServer řešení integrované přímo do software XenCenter, popřípadě řešení postavené na technologii Citrix ICA klient.

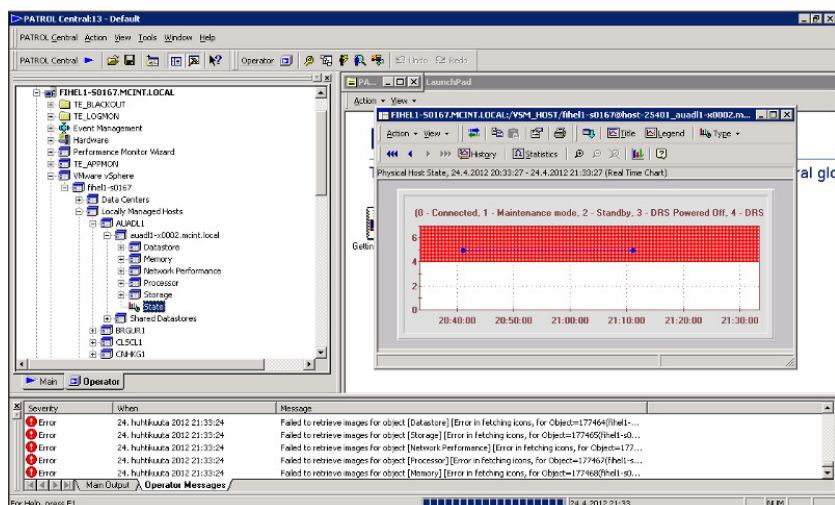
### 3.2 Citrix XenApp

Ne vždy je možné používat přímý přístup k prostředkům serverů. Zvláště v případě, že požadovaná bezpečnost spravovaného systému je tak velká, že není možné otevřít firewall k jumpointu, popřípadě chceme zabezpečit i samotnou možnost použít schránku ke kopírování textů či pořízení snímků obrazovky.

XenApp je nástroj vyvinutý společností Citrix Systems, který umožňuje uživatelům připojit se k jejich aplikacím pomocí tenkého klienta. XenApp hostuje aplikace na centrálním serveru s tím, že v reálném čase streamuje veškeré obrazové a periferní data přes síť k uživatelům. Zároveň lze nastavit na serveru vysokou úroveň zabezpečení tak, aby nedošlo k žádné kompromitaci dat.

Citrix ICA klient je plugin do webového prohlížeče, který umožňuje využívat služeb poskytovaných serveru platformy Citrix XenApp. Na obrázku 2 můžeme vidět základní





Obrázek 3: Rozhraní Patrol Central Operator

obrazovku tenkého klienta s několika ikonkami aplikací vypropagovaných z centrálního serveru.

Tento produkt je v Unixovém týmu konkrétně používán k přístupu do vývojářského prostředí BITS, a k administraci švédského virtualizačního prostředí.

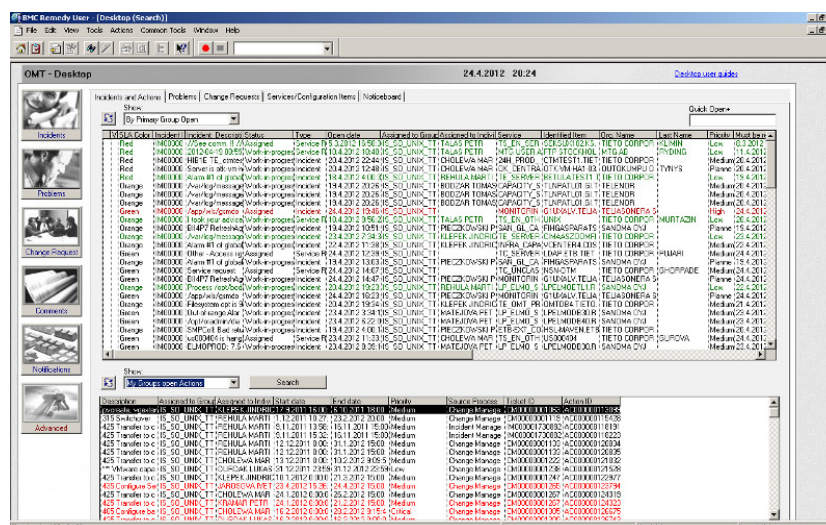
### 3.3 Monitoring

Servery a aplikace na nich běžící jsou sledovány několika možnými způsoby, především však softwarem firmy BMC - Patrol [2], popřípadě open source řešeními – Nagios [10] nebo nástrojem monit. Jmenované poslední dva jsou však použity přibližně v 1% celkové infrastruktury a to většinou jen jakou podpůrné nástroje. O správné nastavení funkcí monitoringu serverů se stará specializovaný tým.

#### BMC Patrol

BMC Patrol je monitorovací systém vyvinutý firmou BMC Software. Skládá se ze tří samostatných komponent. První z nich je Agent. Ten je nainstalován na každý monitorovaný systém. Další komponentou je takzvaný RT, neboli RealTime server. Ten sbírá informace z jednotlivých agentů a dále je předává centrálnímu RT serveru. RT servery tvoří takto stromovou strukturu. Kořen stromu je dále napojen na další infrastrukturu, tedy tiketovací systém a poslední komponentu. Tou je konzolový server, nazývaný Patrol Central Operator (obrázek 3). Ten ve formě tlustého klienta zajišťuje spojení s RT servery, ze kterých dokáže načítat data a zobrazovat je v reálném čase uživatelům.

V případě, že tedy dojde k poruše na nějaké sledované části infrastruktury, je automaticky tento problém eskalován přes monitorovací infrastrukturu tak, že je vytvořen incident tiket, a poslán na první vrstvu podpory. Zde dojde k vyhodnocení problému. Specialista z první vrstvy se připojí na konzolový server a zkontroluje status. Pokud ani



Obrázek 4: Rozhraní nástroje BMC Remedy User

po předem definovaném časovém úseku nedojde k zaniknutí problému, je porucha vyhodnocena jako relevantní. Následně je již na specialistovi, zda je v jeho silách poruchu odstranit, nebo využít možnosti eskalovat tiket na odpovídající tým z druhé vrstvy podpory.

### 3.4 Tikety

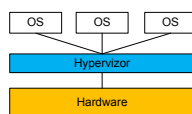
Podle modelu ITIL je každý požadavek ať už automatický, či ručně vytvořený interpretován jako takzvaný Tiket.

K manipulaci s těmito Tikety je používán nástroj firmy BMC, Remedy User [3]. Ten je plně integrován podle požadavků na korporátní procesy. Každý Tiket obsahuje informace o tom, kdo jej vytvořil, jaké je zadání problému, do kdy musí být Tiket vyřešen – takzvané SLA, neboli odkaz na dohodu o úrovni služeb a dále informace o tom, kdo na problému pracoval, pracovní deník, odkazy na problémy a další informace nutné k jeho řešení.

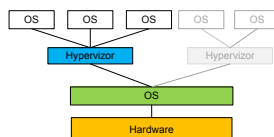
Tikety se dělí podle procesů, ke kterým patří na Incidenty, Problémové tikety a Tikety změn, takzvané Change. Nezávisle na tom můžeme vytvořit navíc takzvané akční tikety, které reprezentují konkrétní předem definované způsoby řešení nějakého problému a bývají součástí především změnového nebo problémového managementu.

BMC Remedy User dále umožňuje i vyhledávání, takže specialista pracující na některém z incidentů může zjistit, zda se nejedná o nějaký opakující se problém, popřípadě zda na stejném typu incidentu nepracuje někdo další, což může v jistých případech urychlit a zjednodušit práci.

Rozhraní programu BMC Remedy User můžeme vidět na obrázku 4.



Obrázek 5: Hypervizor typu 1 (bare-metal)



Obrázek 6: Hypervizor typu 2

### 3.5 Virtualizace

V současné době je ve velké oblibě virtualizace. Jedná se o abstrakci prostředků hardwaru na prostředky softwarové. Virtualizační software se pak dále chová jako by se jednalo o skutečný hardware. Software spuštěný na takovémto hardware je od něj izolován a používá pouze část jeho prostředků.

V terminologii virtualizace nazýváme virtualizovaný stroj jako *guest* (česky *host*), skutečný hardware pak jako *host* (česky *hostitel*). Software, který se stará o virtualizaci pak nazýváme *hypervisor*.

Virtualizace hardwaru však není jeho emulací. Hypervisor nedokáže emulovat nějaký kus hardware, který reálně na hostiteli nemáme. Ne všechen hardware je však schopný virtualizovat. K tomu aby jsme mohli úspěšně použít konkrétní počítač, musí splňovat podmínky definované Gerald Popekem and Robertem Goldbergem v jejich článku o virtualizování třetí generace architektur [12]. Moderní servery však disponují nejen těmito prostředky, ale většinou i prostředky pro hardwarově asistovanou virtualizaci. Na takovémto hardware není pak například nutné na úrovni hypervisoru implementovat složité algoritmy pro ošetření privilegovaných volání procesoru, ale můžeme se spolehnout na to, že nám jej zabezpečí hardware.

Hypervisory dělíme na takzvané hypervizory *Typu 1*, neboli **bare-metal** a na hypervizory *Typu 2*, neboli **hostované**.

První typ je spuštěn přímo nad reálným hardware a využívá přímo jeho prostředky. Výhodou prvního typu je relativně vyšší výkon díky možnostem využití celého potenciálu hardware. Nevýhodou je, že sám hypervisor musí mít veškeré ovladače pro daný hardware. Schéma tohoto hypervisoru pokrývá obrázek 5).

Druhý typ je spuštěn jako proces nad nějakým konkrétním operačním systémem a využívá pouze prostředky přidělené tímto konkrétním operačním systémem. Druhý typ hypervisoru je na OS plně závislý (včetně jeho omezení). Výhodou však může být, že nepotřebujeme žádné speciální ovladače, a můžeme spustit více instancí daného hypervisoru na jediném hostiteli. Schéma můžeme vidět na obrázku 6.

## Nativní virtualizace

Ta je někdy také nazývaná plná virtualizace. Hypervisor nabízí veškeré prostředky pro běh nemodifikovaného operačního systému.

## Částečná virtualizace

U tohoto typu virtualizace jsou ne všechny prostředky hostitelského systému dány k dispozici hostovi. Může se jednat jak o instrukce procesoru tak o konkrétní hardwarové prostředky. Hostovaný systém tak může vyžadovat modifikace kódu, aby bylo možné jej na takovémto hostiteli spustit.

## Paravirtualizace

V tomto případě není simulováno konkrétní hardwarové prostředí, ale pouze vytvářen jakýsi kontejner (doména) nad hardware tak, aby byly procesy od sebe navzájem izolovány jako by byly spuštěny nad samostatným hardware. Takovéto programy vyžadují specifickou modifikaci kódu, aby byly vůbec spustitelné v paravirtualizačním prostředí. Obvykle je to řešeno modifikací jádra operačního systému a základních systémových knihoven.

Důvodů k virtualizování serverů může být mnoho. Nejčastějším z nich je požadavek na rychlou instalaci. V situaci, kdy objednání a dodání nového serveru může zabrat i několik týdnů, je instalace serveru na virtuální platformu otázkou několika málo hodin. Pokud navíc použijeme nějaký template, čili předem připravený obraz hotového serveru, může se instalace zkrátit až na řády několik minut. Dalším obvyklým důvodem virtualizování serverů je vysoký výkon a cena hardwaru. Seryvery dnes, až na malé výjimky, obvykle několikanásobně výkonově překračují požadavky softwaru. Díky tomu, že jednotlivé virtuální servery mohou mezi sebou sdílet prostředky jednoho serveru fyzického, můžeme umístěním na jeden fyzický hardware ušetřit pro zákazníky důležité finance, které můžou věnovat místo na hardware do jiného odvětví.

## Virtualizace ve společnosti Tieto

Ve společnosti Tieto se ve většině případů používá především plná virtualizace prvního typu (viz 3.5) a to produkt firmy VMware, vSphere [16]. Ostatní, minoritně používané, prostředky k virtualizaci jsou Enterprise virtualizace společnosti RedHat[14] a Citrix XenServer[4], ty i pro jejich mnohem nižší náklady na provoz nejsou doposud tak populární jako konkurenční produkt a to především kvůli jejich ne tak dokonalé funkčnosti.

Struktura architektury VMware vSphere je následující. Na hostitelích je nainstalován hypervisor VMware ESX. Následně jsou hostitelé po síti propojeni do clusterů, umožňující živé migrace mezi jednotlivými hostiteli, dynamické sdílení prostředků, funkce vysoké dostupnosti, funkce distribuovaných síťových switchů a další funkcionalitu. Ke každému hostiteli je připojeno několik diskových polí. Na ty se ukládají obrazy virtuálních strojů,

případně instalační obrazy. Neposlední důležitou komponentou je takzvaný vCenter Server. Jedná se o dedikovaný server, na kterém je nainstalován software spravující funkce celého clusteru, případně samostatných hostitelů. Ten skrze agenta ovládá jednotlivé hypervizory. Další komponentou architektury je databáze. Do té se ukládají veškeré informace o stavu clusteru a rovněž logy z jeho činnosti.

Ke správě celé architektury se používá software **vSphere Client**. Jedná se o tlustého klienta umožňujícího nám plnou kontrolu všech připojených hostitelů a hostů. Rovněž umožňuje připojení na virtuální monitory jednotlivých virtuálních strojů tak, jako kdyby jsme byli u fyzického monitoru toho konkrétního hosta.

Další možností ovládání je VMware vSphere **PowerCLI**. Jedná se o rozšíření skriptovacího nástroje PowerShell [8]. Umožňuje nám automatizovat všechny prvky API, platformy vSphere pomocí skriptů a je mocným nástrojem pro provádění úkolů, které by byly při použití pouze klasického vSphere klienta vysoce časově nebo prostředkově náročné.

Posledním významným používaným nástrojem je software VKernel VOPS (vOperations) [15]. Ten poskytuje silné možnosti v oboru analýzy a reportování celé architektury vSphere. Umožňuje generovat analýzy využití prostředků, předpovědi zatížení jednotlivých clusterů, seznamy virtuálních strojů včetně detailů a má dalších mnoho užitečných funkcí.

## 4 Řešené úkoly - UNIX

V následující kapitole uvádím vybrané problémy řešené během praxe z oboru správy Unixového prostředí v rozsahu od jednoduchých po vysoce časově náročné.

### 4.1 Plný souborový systém

Ne vždy se při procesu návrhu nového serveru podaří vhodně navrhnout rozložení a velikosti souborového systému, případně může nastat situace, kdy bylo vše navrženo správně pro běžné používání, ale nepočítalo se s krajními případy. Tehdy dojde zákonitě po jisté nedefinované době k zahlcení některého z špatně navržených souborových systémů a je nutno provést kroky vedoucí k uvolnění místa. Tím může být promazání nepotřebných souborů, provedení komprimace nových souborů nebo spuštění předem definovaných čistících skriptů.

V případě, že se nejedná jen o jednorázové zaplnění, kdy by navrhované kroky vedly pouze k dočasnému řešení, dojde k překlopení na změnový management, a je nutno objednat a přidat nové disky.

Zaplnění disků může rovněž vyvolat proces problémového managementu, kdy je nutné vyřešit zdroj problémů – proč se vlastně disk zaplnil. Výstupem by měl být důvod – například *špatně navržená aplikace, uživatelé si tam nahráli soubor, a podobně* a také řešení v podobě změnového managementu – *opravme aplikaci, zakažme uživatelům nahrávat velké soubory, přidejme disky, atd.*

Konkrétní příklad můžeme vidět ve výpisu 1. Došlo k zaplnění disku v důsledku intenzivního logování aplikace. Log byl manuálně odrotován a zkomprimován. Místo bylo uvolněno.

---

```
# cd /var/log
# find . -size +10000 -type f -exec ls -lh {} \;
-rw-r----- 1 root wheel 10G Jan 1 15:24 xferlog
# fuser xferlog
xferlog: 29689
# cat xferlog | gzip -9 > xferlog.gz && :> xferlog

# df -h | grep var
/dev/wd0f 39.4G 13.8G 23.6G 37% /var
```

---

Výpis 1: Manuální řešení problému plného disku

### 4.2 Rozšíření místa na disku

Disky můžeme dělit několika způsoby. Buď to použijeme klasickou tabulku oddílů, známou již z dob DOSu, kdy jednotlivé oblasti disku zabírají pevně stanovený rozsah bloků, nebo můžeme použít některý z manažerů logických disků, jako je LVM.

Klasický způsob přináší značné komplikace, pokud chceme s oddíly jakkoliv manipulovat. Musíme celý oddíl smazat, data předtím někam odmigrovat a vytvořit jej zcela

znova a data opět nahrát zpět. To může být (a je) nepříjemné v prostředích, kdy služby musí být dostupné většinu času.

Proto se na serverech používá LVM. To nám dělí disky na tři vrstvy. Fyzický oddíl – PV (Physical Volume), který je reprezentován konkrétním blokovým zařízením. Další vrstvou je skupina oddílů, neboli Volume Group – VG, ta se vytváří nad jedním nebo více fyzickým oddílem a jedná se prakticky o jakýsi pool dostupného volného místa. Nad VG následně vytváříme logické oddíly, neboli LV – Logical Volume. LV reprezentují konečné blokové zařízení, nad kterým můžeme dále vytvářet souborové systémy.

Rozšíření takové LV pak není žádný problém, pokud je ve VG místo, pouze spustíme příkaz na rozšíření a následně provedeme i rozšíření souborového systému.

---

```
# zvetseni logicke volume o 10G
lvextend -L+10G /dev/vg_root/lv_data
```

```
# on-line zvetseni FS
resize2fs /dev/vg_root/lv_data
```

---

#### Výpis 2: Rozšíření LVM oddílu

V případě, že v VG není místo, můžeme přidat jeden nebo více PV do této skupiny, čímž celou VG příslušně rozšíříme.

---

```
# vytvoreni nove PV na zarizeni
pvcreate /dev/sdx1
```

```
# rozsireni VG o novy disk
vgextend /dev/vg_root /dev/sdx1
```

---

#### Výpis 3: Přidání zařízení VG

Další možností, dostupnou v současnosti ve stabilní verzi pouze v Solarisu a BSD je použití souborového systému ZFS. Ten v sobě integruje manažer logických disků a high-performance souborový systém podporující deduplikaci dat, snapshoty, transparentní kompresi, šifrování a jiné možnosti. Více o ZFS se můžeme dočíst na stránkách společnosti Oracle [zfsora].

V případě ZFS je rozšíření souborového systému triviální, jelikož ten díky používání takzvaných poolů namísto klasické interpretace oddílů zpřístupní nový disk do poolu okamžitě.

---

```
zpool add striped c1d2
```

---

#### Výpis 4: Přidání prostoru při použití ZFS

## 4.3 Spadlé procesy, služby

Ne vždy fungují všechny služby bezproblémově. Vlivem špatně napsané aplikace, případně chybě hardware, nebo nějaké blíže nespecifikované chybě dojde k pádu nějaké aplikace. V takovém případě dostaneme z monitoringu varování, že některá z instancí daného procesu má podlimitní počet potomků. Je tedy nutno se přihlásit na server, provést kontrolu

jaké procesy jsou spuštěny. Pokud sledovaný proces neběží, je nutno jej spustit, pokud běží, je nutno zkontrolovat v jakém stavu se nachází. V případě velkých problémů je nutno projít logy aplikace, popřípadě provést **trace** nebo **debugování** procesu. Dlouhodobý stav výpadku aplikací může vést až k problémovému managementu.

## 4.4 Správa uživatelských účtů

Může se jednat o přidávání, mazání případně úpravu uživatelských účtů. Do firmy Tieto každým měsícem přicházejí noví uživatelé a jiní jsou propouštěni. Rovněž zákazníci potřebují čas od času přístup na své servery z rozličných důvodů. Jedním z nich může být i audit externí společností, při kterém se ověřuje, zda je zabezpečení serverů dostatečné a odpovídá aktuálním standardům.

Pokud se nejedná o příliš velké množství uživatelů, provádí se správa ručně. Přihlásíme se na server, spustíme příkaz pro přidání uživatele, nastavíme mu heslo, případně další propriety a zašleme mu heslo elektronickou poštou.

Pokud se jedná o velké množství uživatelů, případně serverů, je vhodné si napsat na tento úkol skript. Ve výpisu 5 můžeme vidět část takového skriptu. Tento úsek skriptu řeší přidání uživatele do skupiny sudo na vzdáleném serveru. Celý skript je napsaný v kombinaci jazyků Expect a Unix shell řešící přidání uživatelů na jeden až více serverů. Automaticky se přihlásí na server jako privilegovaný uživatel, provede operace přidání a nastavení oprávnění. Po skončení skriptu pak jen zbývá rozeslat hesla příslušným uživatelům. Tento skript je plně ovladatelný konfiguračními proměnnými, které zajišťují možnost změnit heslo superuživatele, používat předdefinované hesla namísto automaticky generovaných a jiné další detaily. Celý skript můžeme nalézt na CD tištěné verze této bakalářské práce.

---

```
spawn ssh -l root ${ip}
expect {
  stty -echo
  "*yes/no*" { send "yes\r"; exp_continue }
  "*assword:" { send "${PW}\r"; exp_continue }
  stty echo
  "Last*" { exp_continue }
  "*#" {
    send -- "SISAT=$(grep -n \"^%sudo\" /etc/sudoers | tail -n 1 | cut -d: -f1)\r"
    send -- "if [ 0$${SISAT} -eq 0 ]; then\r"
    expect ">*"
    send -- "cat <<SUDO2 >> /etc/sudoers\r"
    expect ">*"
    send -- "## ---- ADDED_BY_SKRIPTOS_BEGIN ----\r"
    expect ">*"
    send -- "### Allows people in group wheel to run all commands\r"
    expect ">*"
    send -- "%sudo_ALL=(ALL) ALL\r"
    expect ">*"
    send -- "## ---- ADDED_BY_SKRIPTOS_END ----\r"
    expect ">*"
    send -- "SUDO2\r"
    expect ">*"
  }
}
```



```

send -- "fi\r"
expect "*"
send -- "ISGROUP=\$(grep -n \"sudo:\" /etc/group | tail -n 1 | cut -d: -f1)\r"
send -- "if \[0\$\{ISGROUP\} -eq 0\]; then\r"
expect ">*"
send -- "groupadd sudo\r"
expect ">*"
send -- "fi\r"
expect "***"
send -- "logout\r"
expect eof
}
}
EXPECT2

```

#### Výpis 5: Část skriptu pro vytváření uživatelů

Za zmínku stojí, že v době psaní této práce se několik serverů převedlo pod správu nástroje AARM, vyvíjeného firmou Oracle, který umožňuje správu a ovládání uživatelských účtů přes webový formulář, bez nutnosti hlásit se fyzicky na servery. Až budou všechny servery převedeny pod tento nástroj stane se používání vlastních skriptů zastaralým.

## 4.5 Audit

Jak již bylo zmíněno v jedné z kapitol, dochází pravidelně k kontrolám bezpečnosti serverů. To provádějí buďto specializované společnosti, kterým je jen umožněn přístup k serverům, nebo je doručen skript, který je nutno spustit a auditorské společnosti dodat pouze výsledky. Úkolem tedy je zajistit spuštění konkrétního skriptu na serverech tak, aby výsledky byly snadno dostupné. Jelikož se jedná o velké množství serverů, opět byl vytvořen skript v jazyce Expect, který je schopen takovýto úkol vykonat.

```

spawn ssh -l $user $host
expect {
  "*yes/no*" { send "yes\r"; exp_continue }
  "*password:*" { send "$userpw\r"; exp_continue }
  "passwd:.*all*" { exp_continue }
  "*denied*" { puts "ERROR: Password for $user is incorrect."; exit 0 }
  -re "\[%$#>\]" { incr logged_in 1 }
  -re "..*" {
    if { !$logged_in && $motd_counter <= $motd_max } {
      incr motd_counter 1
      exp_continue;
    }
  }
}

```

#### Výpis 6: Část skriptu řešící připojení na server

Část skriptu řešící připojení na server a spuštění příkazu je ve výpisu 6. Nejdříve vytvoříme potomka ssh procesu. Následně je nutné otestovat, zda server neposlal žádost o akceptování ssh klíče. Následně se pokusíme odeslat heslo. V případě chybného hesla končíme skript. Jinak zjistíme, zda máme prompt a pokud ne, je třeba pokračovat ve vyhodnocování doku neujistíme, jaký je problém, nejvíce však `motd_max` pokusů.

## 4.6 Instalace nových serverů

Instalace nových serverů jsou významnou součástí změnového managementu. Rovněž jsou důležité pro vybudování infrastruktury pro zákaznická prostředí.

Fáze plánování je provedena odpovědným týmem, který projedná veškeré podrobnosti se zákazníkem a podle nich sestaví změnový tiket. Ten je následně předán na Unixovou skupinu, kde proběhne samotná fáze vykonání instalace.

Ta probíhá vzdáleně, přes některý z nástrojů pro vzdálenou kontrolu. Buďto přes tenkého klienta v prohlížeči, pokud se jedná o management rozhraní integrované v serveru, nebo přes program VMware vSphere Klient, pokud se jedná o virtuální server.

Instalace probíhá v několika fázích. V první fázi je nutno zajistit připojení instalačního média. To je buďto zajištěno již před spuštěním instalace připojením takzvaného instalačního kabelu, což je speciální dedikovaná VLAN, obsahující PXE server a FTP server se soubory nutnými pro instalaci, nebo je nutno připojit CD přes virtuální CD adaptér serveru. Z osobní zkušenosti můžu říci, že při připojení CD je instalace mnohem rychlejší, jelikož není využívána již tak přetížená síť. Další fáze je samotná instalace, kdy jsou v instalačním programu nastaveny parametry jako rozložení disků, parametry spuštění, nastavení zabezpečení a požadované součásti systému. V další fázi dochází k dokončení konfigurace a instalace doplňků a aplikací serveru.

Nutné konfigurační změny jsou:

- Vypnutí X serveru.

To se provádí nastavením parametru `initdefault` na hodnotu 3, což nastaví výchozí `runlevel` na spuštění bez grafického prostředí.

- Zakázání kláves `Ctrl–Alt–Del`.

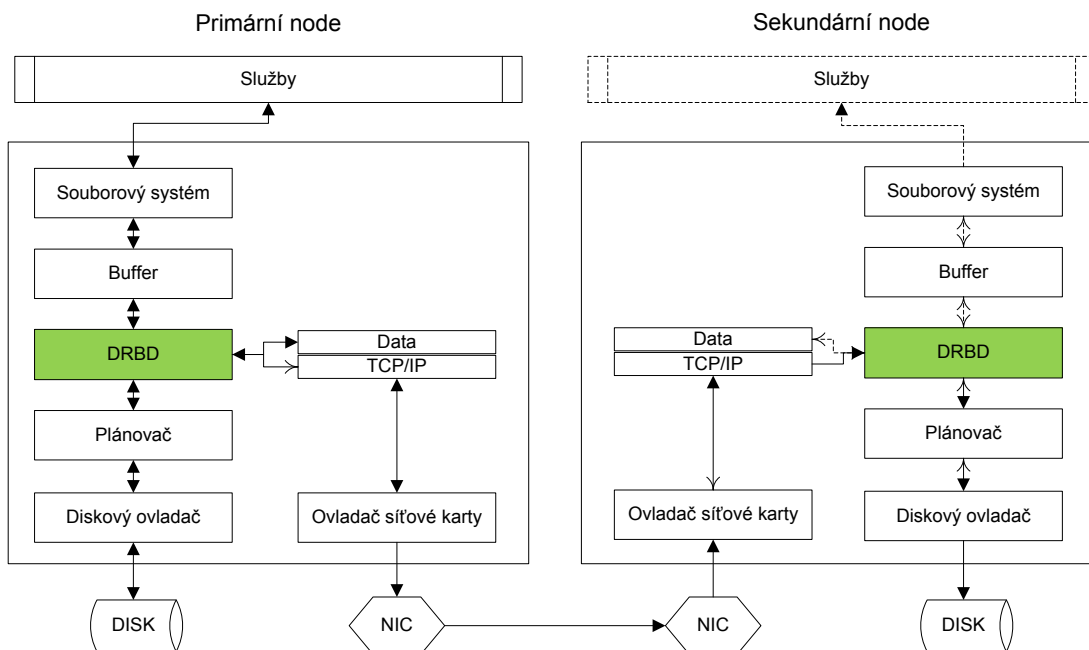
Unixové servery se liší od platformy Windows i v ohledech klávesových zkratk. Je proto nutné zajistit, aby při stisku `Ctrl–Alt–Del` nedošlo k restartování serveru, jak je tomu nastaveno ve výchozí hodnotě. Tato zkratka by na platformě windows vyvolala přihlašovací obrazovku, ale na Unixu by to mohlo mít fatální následky. Je nutné, aby byla tato zkratka ignorována, nebo pouze rozsvítila vypnutou obrazovku. To se nastavuje v souboru `/etc/inittab` zakomentováním příslušné zkratky.

- Instalace zálohovacího agenta.

Jelikož agent se nedistribuje jako balík pro operační systém, ale pouze jako sada souborů, je třeba provést některé části instalace ručně. Je třeba ručně editovat soubor servisů a přidat tam záznam o nové službě, dále nakopírovat spouštěcí skripty na správné místo a rovněž nastavit routování pro síťovou kartu dedikovanou pro zálohování.

- Instalace monitorovacího agenta

Ta se provádí spuštěním instalačního programu přes webový prohlížeč. Je nutno zadat přihlašovací údaje na server, a instalátor se již postará o veškerou zábavu. Po skončení instalace je třeba zkontrolovat, zda monitorovací agent běží. Může se



Obrázek 7: Schéma funkcionality DRBD

totiž stát, že na serveru chybí některá sdílená knihovna a agent se tudíž nespustil, nebo vůbec nenainstaloval, aniž by to instalátor zjistil. V takovém případě je nutné knihovna doinstalovat a instalátor znovu spustit.

Po těchto provedených změnách jsou ještě odeslány akční tikety na týmy, jež nastaví a zprovozní monitoring a zálohy. Následně je server připraven k používání.

## 4.7 Cluster

V některých případech je požadavek na stabilitu služby maximální. Tehdy je nutné zvolit prostředky, jež zajistí, aby při fyzickém pádu serveru byla stále zajištěna maximální dostupnost služeb.

## 4.8 DRBD

DRBD je ovladač blokového zařízení, umožňující vytvořit sdílený diskový prostor pro vysoce dostupné clustery. Principem je vytvoření zrcadleného obrazu disků mezi jednotlivými stanicemi na síti. Můžeme jej také zjednodušeně označit jako RAID1 přes síť. Výhodou tohoto řešení je snadná konfigurace a poměrně vysoká stabilita dat.

Na obrázku 7 můžeme vidět principiální rozložení. Pokud si operační systém požádá o blok dat, jsou tyto data přečtena z lokálního disku. Při zápisu dochází opět nejdříve k zápisu na primární (lokální) disk, následně jdou data odeslána po síti na sekundární disk. V závislosti na konfiguraci může být tato operace buď synchronní, nebo asynchronní.

Výhodou DRBD je, že se jedná čistě o ovladač blokového zařízení. Neobsahuje tak sám osobě žádný souborový systém a my na něj můžeme aplikovat libovolný dostupný v dané distribuci.

Během své praxe jsem DRBD nastavoval celkem třikrát. Dvakrát v režimu jednoho primárního uzlu, což je standardní režim a jednou v režimu více primárních uzlů.

Nastavení jednoho primárního uzlu je celkem triviální. Jediné, co musíme zajistit je, aby v případě výpadku jednoho z uzlů byl ten první odstaven. K tomu se používá metoda STONITH, což je zkratka anglického Shoot Other Node In The Head, neboli střel druhý node do hlavy. Můžeme rovněž nastavit clusterovací software, který se nám stará o aplikace, aby se o likvidaci spadlého node postaral sám. V takovém případě nenastavujeme STONITH v rámci DRBD, ale až na úrovni aplikačního clusteru.

Režim dvou uzlů je komplikovanější, toto nastavení vyžadovalo speciální podporu ze strany aplikačního clusteru a také podporu ze strany samotného souborového systému. K implementaci byl nakonec zvolen souborový systém firmy RedHat, GFS2 – Global File System. A ke správě logických oddílů bylo zvoleno clusterovací LVM. Nastavení probíhalo obdobně jako při režimu jednoho primárního uzlu, s tím rozdílem, že již od začátku byly všechny služby ohledně disků konfigurovány jako zdvojené. Za zmínku stojí, že toto řešení je možné pouze s použitím aplikačního clusteru založeného na projektu Pacemaker.

## 4.9 Pacemaker, Corosync a RedHat Cluster Suite

Red Hat Cluster Suite je skupina softwarových balíčků integrovaných do distribuce Redhat Enterprise Linux. Obsahuje démona pro heartbeat, cluster manager a resource manager. Konfigurace se provádí editací XML souboru *cluster.conf*, který obsahuje veškerou konfiguraci clusteru. Následně je třeba ručně, nebo příkazem roz distribuovat konfiguraci na všechny ostatní nody clusteru. Ve výpise 7 můžeme vidět základní nastavení clusteru obsahující jednu službu. Ta je součástí jedné failover domény, tedy skupiny serverů, které mezi sebou sdílejí služby, takže při výpadku bude automaticky restartována.

```
<rm>
  <services>
    <service autostart="1" checkinterval="15" failoverdomain="apache" id="1" name="apachesvc" \
      userscript="/etc/cluster/apachesvc">
      <ip address="1.2.3.4" monitor_link="1"/>
    </service>
  </services>
  <failoverdomains>
    <failoverdomain id="0" name="apache" ordered="yes" restricted="no">
      <failoverdomainnode id="0" name="host1"/>
      <failoverdomainnode id="1" name="host2"/>
    </failoverdomain>
  </failoverdomains>
</rm>
```

Výpis 7: Úsek konfigurace služby RedHat Clusteru

Pacemaker je OpenSource resource manager používaný v kombinaci s cluster managerem Corosync. Jedná se o vysoce kvalitní řešení jak sestavit cluster. Umožňuje snadné nastavení pomocí příkazové řádky. Rovněž obsahuje přímou podporu síťových souborových systémů GFS2, OCFS, a DRBD řešení. Ve výpise 8 můžeme vidět příklad přidání nové služby do konfigurace clusteru. Oproti nutnosti přidat ručně celý blok XML u Red-Hat Clusteru se jedná o triviální operaci.

---

```
bash# crm configure
CRM# primitive failover--apache lsb::apache op monitor interval=15s
CRM# verify
CRM# end
```

---

Výpis 8: Přidání služby apache do clusteru

## 4.10 Veritas Cluster

Veritas Cluster Server je kompletní řešení pro vysokou dostupnost aplikací vyvíjený firmou Symantec. Obsahuje proprietární řešení síťového souborového systému a blokového zařízení, a širokou podporu skriptů pro jednotlivé aplikace, jako je Oracle databáze, nebo aplikační server Tomcat. Tento cluster se však ve společnosti Tieto příliš nepoužívá, vzhledem k jeho vysoké ceně. To je dle mého názoru ovšem škoda, jelikož v porovnání s předchozími popsányými řešeními nabízí mnohem větší možnosti v oblasti konfigurace, funkcionalit a administrace.

## 5 Řešené úkoly - Virtualizace

Unixový tým má na starosti několik virtualizačních prostředí založených na platformě VMware Vsphere. Hlavních z nich je takzvané kapacitní prostředí, které obsahuje virtuální hosty rozličného množství zákazníků, a v době psaní této práce se skládalo přibližně z 50 hostitelů a 2000 hostovaných virtuálních strojů. Následující kapitoly obsahují popis některých řešených problémů těchto prostředí od nejjednoduššího po velmi náročné.

### 5.1 Alokace

Při instalaci serveru přicházejí rovněž požadavky na vytvoření základního síťového prostředí. Je proto nutno vytvořit prázdný obraz serveru v prostředí VMware. To je celkem triviální operace, kdy je nutno se přihlásit na vCenter server prostředí VMware a provést vytvoření nové virtuálního stroje.

Dalším úkolem je alokace VLAN. Tak se skládá ze dvou kroků. První udělá tým starající se o sítě, kdy VLAN zpřístupní na přepínačích připojených k hostitelích. Následně Unix tým přidá VLAN do prostředí VMware.

### 5.2 Reporty

Je dobré vědět, kolik prostředků je aktuálně využito, jak z důvodu, že je nutno tyto prostředky účtovat zákazníkům, tak i z důvodu, že potřebujeme naplánovat vhodné rozložení nově alokovaných serverů.

Jedním z nástrojů pro vytváření plnohodnotných statistik je VKernel Operations Suite. Jedná se o takzvanou virtuální appliance, tedy již předpřipravený obraz virtuálního systému. Ten se nainstuluje do virtuálního prostředí, a po provedení základní konfigurace je schopen z interních logů ESXů a vlastních naschromážděných dat vytvořit plnohodnotné statistiky. Z parametrů které můžeme sledovat je nejvýznamnější paměť, využití CPU, a využití diskového prostoru.

Další možností, jak vygenerovat nějaké použitelné data je použití PowerCLI. To nám nabízí velké možnosti jak pracovat s API VMware vSphere. Následující krátký výpis 9 umožňuje vypsát seznam virtuálek v clusteru Test1, a vypsát jejich síťové karty včetně MAC adres, což například GUI vSphere klienta jednoduše neumožňuje.

---

```
$credCosmgmt = Get-Credential -Credential admin
Connect-VIServer -Credential $credCosmgmt -Server vcenter1,vcenter3
Get-VM -Location Test1 | Get-NetworkAdapter | Select-Object -Property Parent,Name,Type,
NetworkName,MacAddress
```

---

Výpis 9: Vytvoření seznamu virtuálního prostředí pomocí PowerCLI

### 5.3 Migrace serverů

Migrace můžou probíhat jak mezi jednotlivými Clustery, kdy automatický manažer řídící rozdělení prostředků clusteru rozhodne, že je jeden z nodů clusteru přetížen a je třeba jej

uvolnit. Můžeme také provést ruční migraci prostředků. Můžeme provádět migrace také mezi jednotlivými datovými úložišti.

Občas je třeba provést přesun velkého množství virtuálních serverů najednou, což by v GUI klientu zabralo množství času a prostředků technika. Vhodnější je použití skriptu v PowerCLI, který dokáže přesunout zadaný seznam serverů několika málo příkazy. Výpis 10 zobrazuje úseky kódu nutné k provedení migrace.

---

```
# nacteme seznam virtualek
$vm = Get-VM -Name (Get-Content H:\virtualky.txt)

# muzeme jej i vypsat na obrazovku
$vm

# zjistime volne misto
($vm | Get-HardDisk | Measure-Object CapacityKB -sum).Sum/(1024*1024)

# vybereme vhodny datastore
Get-Datastore | sort FreeSpaceMB

# presuneme virtualky
Move-VM -VM $vm -Datastore svn_storage2_455GB
```

---

Výpis 10: Migrace serverů mezi úložišti

## 5.4 Nové prostředí a P2V konverze

Postavení nového VMware prostředí se musí řídit několika pravidly. Musí být zajištěna dostatečná kapacita hostitelů a to jak v ohledu prostředků serveru, tak ze strany sítě. Ze strany sítě je pak nutný požadavek na dostatečný počet síťových karet. Vyžadovány jsou minimálně čtyři, dvě pro produkční prostředí – ty jsou spojeny do bondu a chovají se jako jedna a další síťová karta pro management a jedna pro interní potřeby clusteru.

Součástí vybudování nového prostředí bývá i konverze fyzických serverů do virtuálního prostředí. To se provádí pomocí nástroje VMware converter. Ten dokáže převést data uložená na fyzickém serveru včetně všech nastavení do obrazu virtuálního stroje, který můžeme následně spustit na nějakém hostiteli.

## 5.5 Disaster recovery, MIM

MIM, neboli Major Incident Management je proces, mající kritický vliv na větší část infrastruktury. Během své praxe jsem měl možnost podílet se na obnově infrastruktury po jednom kritickém problému, kdy spadlo celé diskové pole, na kterém bylo uloženo na tisíce virtuálních mašin. Bylo třeba obnovit celou infrastrukturu, od instalace serverů, přes nastavení aplikací a znovuvytvoření celého prostředí.

## 6 Zákazníci a soft skills

Během své praxe ve firmě Tieto jsem měl možnost několikrát se setkat s externími uživateli formou jejich požadavků v tiketech, ale také s zástupci společnosti, jíž firma Tieto nabízí své outsourcingové služby.

Komunikace s uživateli je důležitým prvkem práce. Uživatelé mají pocit, že je s nimi komunikováno, jsou spokojenější a spíše doporučí služby společnosti dalším lidem.

Nemálo důležitá je i komunikace přímo se zástupci jiné společnosti, které hodlá Tieto nabídnout své služby. Obvykle je třeba zjistit, jaké prostředky by potřebovali, zjistit jakou mají představu o infrastrukturách, a další parametry. Uživatelé obvykle neznají technické detaily a proto je důležité zjistit od nich co největší množství informací a na základě něj následně navrhnout cílovou infrastrukturu. Vhodné je pak zkonzultovat s nimi zjednodušené diagramy infrastruktury a sítí, a podle toho navrhnout další parametry. Během procesu je třeba zahrnovat odborníky z dalších odvětví, jako jsou sítě, úložiště, databáze a jiné. Iteračním postupem se následně dopracujeme k výsledku, který bude nejvhodnější pro uživatele – zákazníka a rovněž technicky správný. Na základě toho je pak navrženo a postaveno konkrétní technické řešení.



## 7 Zhodnocení praxe

### 7.1 Znalosti uplatněné

Vysoká škola Báňská v oboru Informatika a výpočetní technika nenabízí mnoho předmětů zaměřených na Unixové prostředí ani které by se zabíraly virtualizací. Nejvíce mi pomohlo studium předmětu Operační systémy, který se zabírá programováním v Unixu a jazyce C, což mi pomohlo se zorientovat v tomto prostředí a pochopit procesy zde probíhající. Dalším významným předmětem, z jehož repertoáru jsem mohl použít znalosti byl předmět Počítačové sítě a rovněž seminář Cisco CCNA, který jsem absolvoval. Ten mi poskytl obстойný přehled nad počítačovými sítěmi, který byl důležitý při komunikaci s týmem zabývajícím se správou síťové infrastruktury. Rovněž v oblasti clusterů mi byly nápomocny znalosti získané v předmětu Paralelní a distribuované systémy, který obsahuje přehled clustrovacích technologií.

### 7.2 Scházející znalosti a zkušenosti

Mnoho znalostí jsem získal samostudiem. Jakožto dlouholetý uživatel Linuxu jsem rovněž vystřídal mnoho distribucí a měl možnost nahlédnout do mnoha zdrojových kódů, díky používání distribuce Gentoo Linux [7]. Bohužel, během mého studia oboru Informatika a výpočetní technika na Vysoké škole báňské jsem se vyhnul předmětům, jež se ať už jakýmkoliv způsobem zabíraly platformou DotNET, případně PowerShell. Veškeré znalosti v tomto oboru jsem si tedy musel nasbírat během praxe ve firmě Tieto. V této oblasti by stálo za to se ještě vzdělávat. V oblasti virtualizace jsem však získal díky absolvování několika školení a praktickým úkolům slušný přehled, který mi studium nemohlo nabídnout. Vhodným předmětem, který bych rovněž uvítal v průběhu mého studia svém studiu by byl i kurz komunikace ve firemním prostředí a se zákazníky.

## 8 Závěr

Společnosti Tieto je mezinárodní společnost. Z toho plyne také způsob jak byly některé problémy řešeny. Spousta z nich nemohla být vyřešena pouhým jedním individualistou, ale bylo třeba rady a zkušenosti celé skupiny lidí, často z mnoha rozličných týmů. Také jsem měl možnost poznat, že řešení problémů bývá většinou triviální, ale nalézt zdroj tohoto problému bývá většinou velice náročná činnost.

Během své praxe ve společnosti jsem se naučil mnoho věcí z firemního prostředí. Velkým přínosem považuji to, že jsem se měl možnost setkat s systémy a softwarem, který není běžně nikde dostupný. Rovněž komunikace a spolupráce s lidmi z různých koutů světa a různých oborů je velmi přínosná a velmi si ji vážím. Práce v týmu znamená rozvoj komunikačních schopností, které mnohokrát lidem pohybujících se čistě v homogenním IT prostředí chybí. Kolegové mi rovněž byli nápomocní a i já jsem mohl toto oplátit svými novými a originálními nápady k pohledu na řešené problémy.

## Reference

- [1] *Bash, unixový shell, interpret pro příkazový řádek*. URL: <http://www.gnu.org/s/bash/>.
- [2] *BMC Patrol*. URL: <http://www.bmc.com/products/brand/patrol.html>.
- [3] *BMC Remedy Action Request System*. URL: <http://www.bmc.com/products/product-listing/22735072-106757-2391.html>.
- [4] *Citrix XENServer*. URL: <http://www.citrix.com/English/ps2/products/product.asp?contentID=683148>.
- [5] *DRBD, Block devices designed as a building block to form high availability*. URL: <http://www.drbd.org>.
- [6] *Expect, skriptovací jazyk pro automatizaci a testování*. URL: <http://www.nist.gov/el/msid/expect.cfm>.
- [7] *Gentoo Linux*. URL: <http://www.gentoo.org/main/en/about.xml>.
- [8] *Microsoft PowerShell s rozšířením VMware PowerCLI*. URL: <http://www.vmware.org>.
- [9] *Microsoft Visio*. URL: <http://www.microsoft.com>.
- [10] *Nagios*. URL: <http://www.nagios.org/>.
- [11] *Oficiální stránky firmy Tieto Oy*. URL: <http://www.tieto.com/about-us/tieto-in-2-minutes>.
- [12] *Popek and Goldberg virtualization requirements*. URL: [http://en.wikipedia.org/wiki/Popek\\_and\\_Goldberg\\_virtualization\\_requirements](http://en.wikipedia.org/wiki/Popek_and_Goldberg_virtualization_requirements).
- [13] *PuTTY*. URL: <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>.
- [14] *Redhat Enterprise Virtualization*. URL: <http://www.redhat.com/products/virtualization/server/>.
- [15] *vKernel vOPS, nástroj pro monitoring a reporting nad VMware vSphere*. URL: <http://www.vkernel.com/products/voperations-suite/overview>.
- [16] *VMware vSphere, virtualizační architektura*. URL: <http://www.vmware.com/products/vsphere/esxi-and-esx/index.html>.

## A Přílohy k práci

### A.1 Pracovní deník

Tento deník obsahuje významné řešené problémy. Kromě nich je každý týden řešeno množství běžných problémů, jako je zaplnění disku, požadavky uživatelů,

#### Září

Týden 36 Nastavení MySql, Nastavení sendmailu (Prostředí BITS).

Týden 37 Konfigurace+instalace Derby DB+Tomcat aplikačního serveru.

Týden 38 Návrh infraskruktury pro nového zákazníka (cluster databázových serverů a aplikačních serverů, Pro testovací a produkční prostředí). Visio [9].

Týden 39 Skriptování. Expect [6], bash [1] - vzdálený audit serverů, autologin a přenos souborů, kontrola OS, spuštění auditovacích skriptů.

#### Říjen

Týden 40 skriptování, Expect [6], bash [1] - vzdálená správa serverů - management uživatelů (přidání, kontrola oprávnění, likvidace neaktivních).  
Nastavení automatického reportingu - vKernel vOPS [15].

Týden 41 VMware vSphere ESX [16], plánování upgradu s ohledem na minimální downtime (Podle ITIL)  
Jabber cluster - návrh sítí, rozvržení služeb, clustering, vhodná aplikace a platforma.

Týden 42 Návrh sítě + prostředí pro nový ESX [16] cluster lab (vSphere), včetně volby řešení pro redundanci úložiště.

Týden 43 VMware vSphere [16], upgrade prostředí ESX 4.1.0 na ESXi 4.1.0 Update 2.

#### Listopad

Týden 44 Instalace nových serverů.  
Fyzické zapojení nového ESX clusteru (HW) pro lab, instalace clusterovaného storage (DRBD) [5].  
Disaster recovery, analýza zhroutení serveru, analýza logů.

Týden 45 Návrh a instalace clusteru poslední záchrany, požadavek na nezávislost na externích úložištích či dalších službách a sítích včetně volby technologií. Zvoleno DRBD + clvm + GFS + OpenAIS/Corosync, Apache.

Týden 46 VMware vSphere [16], Instalace nových ESX serverů. skriptování, expect [6], bash [1]. Automatické přidávání uživatelů – ladění pro specifika na AIX, HP-UX, Solaris).

Týden 47 Instalace nových Linux serverů a aplikací.  
Příprava P2V migrace (virtualizování fyzického serveru) v rozsahu plánování dle ITIL+základní koordinace kroků.

### **Prosinec**

Týden 48 Disaster recovery, Švédské datacentrum - instalace nových serverů, konfigurace ESX clusteru. powershell [8] skripty pro VMware VSphere.

Týden 49 Disaster recovery, Švédské datacentrum, ladění serverů v rámci ESX clusterů, správa prostředí.

### **Leden**

Týden 2 Reinstalace serverů včetně plánování Change Managementu dle ITIL a jednotlivých akcí.

Týden 3 Plánování změny domény, a jmen serverů, včetně přechíslování sítí.

Týden 4 Přejmenování serverů, aktualizace dokumentace.

### **Únor**

Týden 5 Instalace skupiny serverů, příprava kickstartů.

Týden 6 Interní školení na Editory v Unixu.

Týden 7 Troubleshooting clusteru Veritas.

Týden 8 Návštěva externího zákazníka. Prezentace Unix týmu.

### **Březen**

Týden 9 Plánování VMware prostředí pro vývojářskou skupinu, komunikace se zákazníky.

Týden 10 Reportování několika parametrů virtuální strojů. Nutnost napsat skripty v PowerCLI. Plánování VMware prostředí pro vývojářskou skupinu, komunikace se zákazníky, další iterační fáze.

Týden 11 Řešení běžných popsanych problémů v Unixovém prostředí.

Týden 12 Školení na virtualizační platformu Citrix XenServer.

Týden 13 Seminář RHEV – Redhat Enterprise Virtualization.  
Návrh prostředí pro zákazníka, další fáze.

**Duben**

Týden 14 Nastavení RHEV labu. Základní konfigurace s použitím existujících serverů.

Týden 15 Migrace serverů v rámci prostředí virtualizace. Nastavení VMware Vcentra, příprava na upgrade.

Týden 16 Návštěva externího zákazníka. Presentace Unix a Virtualizačního týmu.